

Stortingets Kommunal- og forvaltningskomité

Vår ref.:

MKF

Dato:

17. mars 2026

Teknas innspill til Dokument 8:119 S (2025-2026) - Representantforslag om digital suverenitet i en urolig tid

Tekna er fagforeningen for over 118 000 naturvitere, teknologer og studenter. Våre medlemmer har høyere utdanning innen Teknisk-naturvitenskapelige fag og representerer viktige kunnskapsmiljøer i Norge, både i offentlig og privat sektor. Mange av våre medlemmer arbeider med utvikling, drift og forvaltning av digitale systemer i offentlig sektor, næringsliv og forskning. På bakgrunn av innspill fra våre utviklermiljøer og teknologer vil Tekna gi følgende vurderinger av representantforslaget om digital suverenitet.

Tekna mener representantforslaget fra SV reiser en viktig og nødvendig diskusjon. Digital infrastruktur er i dag en grunnleggende del av samfunnets styringssystemer og offentlige tjenester. Statlige etater, direktorater, kommuner og andre offentlige virksomheter baserer sentrale funksjoner på plattformer og skytjenester levert av et lite antall globale teknologiselskaper.

Denne utviklingen har skjedd over tid og har i stor grad vært drevet av hensyn til funksjonalitet, kostnadseffektivitet og tilgjengelig kompetanse. Samtidig innebærer konsentrasjonen av digital infrastruktur hos et lite antall globale aktører en strategisk avhengighet som kan få betydning for både beredskap, rettssikkerhet og nasjonal handlefrihet.

Tekna mener derfor det er nødvendig å diskutere hvordan offentlig sektor kan redusere kritiske teknologiske avhengigheter og styrke robustheten i digital infrastruktur.

Samtidig er det viktig at tiltakene bygger på teknologiske realiteter. Digital suverenitet kan ikke forstås som full teknologisk selvforsyning, men som evnen til å redusere kritiske avhengigheter, sikre kontroll over sentrale digitale

funksjoner og opprettholde samfunnskritiske tjenester også i situasjoner der enkelte leverandører eller tjenester faller bort.

1. Stortinget ber regjeringen fastsette digital suverenitet som et overordnet mål i Norges digitaliseringsstrategi.

Tekna støtter at digital suverenitet løftes frem som et strategisk mål i norsk digitaliseringspolitikk.

Digital suverenitet bør forstås som demokratisk og rettsstatlig kontroll over kritisk digital infrastruktur og data. Jurisdiksjonell risiko knyttet til utenlandske leverandører i norsk offentlig sektor har vært kjent i lang tid. Lovgivning som Patriot Act og senere CLOUD Act har gjort det mulig for amerikanske myndigheter å kreve tilgang til data hos amerikanske selskaper, også når dataene tilhører utenlandske borgere og lagres utenfor USA. Digital suverenitet bør derfor også forstås som en korreksjon av tidligere mangelfulle risikovurderinger.

Videre mener Tekna at digital suverenitet bør operasjonaliseres gjennom konkrete teknologiske prinsipper og arkitekturvalg.

Etter Teknas vurdering bør dette særlig omfatte:

- redusert leverandørlåsing
- bruk av åpne standarder og åpne grensesnitt
- portabilitet av data og tjenester
- kontroll over identitets- og tilgangssystemer
- sterkere teknologisk bestillerkompetanse i offentlig sektor

Digitaliseringen av offentlig sektor har over tid ført til omfattende bruk av internasjonale teknologiplattformer. I dag er mange sentrale funksjoner i offentlig sektor knyttet til skytjenester og plattformteknologi levert av et fåtall globale selskaper.

Tekna erfarer at enkelte teknologiske løsninger skaper større praktisk avhengighet enn andre. Kontorstøtte- og samhandlingsplattformer som Office, Teams og Slack er blant de mest utbredte systemene i offentlig sektor. Samtidig finnes det i dag få alternativer som oppleves som fullgode erstatninger for disse løsningene i stor skala.

Et sentralt tiltak for å redusere fremtidig leverandøravhengighet er derfor å legge større vekt på åpne standarder og åpen kildekode ved anskaffelse av ny teknologi.

Tekna mener det er viktig å skille mellom ulike teknologiske løsninger, da noen er mer kritiske enn andre fordi de utgjør grunnlaget for drift av andre systemer.

Særlig følgende områder fremstår som strategisk viktige:

- skyinfrastruktur og plattformtjenester, som brukes til drift av applikasjoner og databehandling
- databaser og analyseplattformer, som er grunnlaget for datadrevne tjenester og kunstig intelligens
- identitets- og tilgangsstyring, som kontrollerer hvem som får tilgang til systemer og data
- kontorstøtte- og samhandlingsplattformer, som brukes av store deler av offentlig sektor i daglig arbeid.

Tekna vil særlig fremheve identitetsforvaltning som en kritisk komponent i mange organisasjoner. Systemer som håndterer autentisering og tilgang, fungerer i praksis som portvakter til virksomhetens øvrige systemer. Kontroll over slike systemer kan derfor være avgjørende for reell kontroll over digital infrastruktur.

Selv om slike systemer ikke nødvendigvis er teknisk mest kritiske, gjør den brede bruken dem til en betydelig avhengighet i praksis.

Tekna vil i den forbindelse også understreke at enkelte kritiske nasjonale tjenester i praksis er avhengige av underliggende skytjenester. Digitale identitets- og autentiseringsløsninger er et eksempel på dette. Hendelser der større skyleverandører har hatt nedetid har vist hvordan bortfall av slike tjenester raskt kan få konsekvenser for sentrale samfunnsfunksjoner. Dette understreker betydningen av å vurdere digital suverenitet også i et beredskapsperspektiv.

2. Stortinget ber regjeringen sikre oppretting av en nasjonal skytjeneste som eies og driftes av det offentlige, for lagring av data og som et offentlig arbeidsverktøy.

Tekna mener det er positivt at representantforslaget løfter spørsmålet om offentlig kontroll over digital infrastruktur. Samtidig er det viktig å presisere hva som menes med begrepet «nasjonal sky», og hvilke konkrete problemer en slik løsning skal løse.

Det er teknologisk mulig å etablere skyinfrastruktur basert på åpne teknologier og standarder. Mange av de grunnleggende teknologiene som brukes i dagens globale skytjenester, er selv basert på åpen kildekode. Samtidig er etablering og drift av en fullverdig skyplattform en svært kompleks oppgave som krever betydelig kompetanse, sikkerhetskapasitet og langsiktig finansiering.

Tekna vil også peke på at eventuell bruk av nasjonale eller europeiske alternativer i privat sektor i stor grad vil avhenge av tre forhold: om løsningene er kostnadsmessig konkurransedyktige, om de oppfyller regulatoriske krav, og om de faktisk løser virksomhetenes behov. Dersom slike løsninger tilfredsstill

disse kriteriene, vil også private virksomheter kunne ta dem i bruk. I en oppstartsperiode vil det imidlertid være sannsynlig at nye løsninger bare oppfyller enkelte av disse kriteriene. Insentiver for å ta i bruk slike løsninger kan derfor være nødvendig i en overgangsfase.

Tekna vil samtidig understreke at spørsmålet ikke nødvendigvis er om staten bør bygge én nasjonal hyperskalaplattform som skal dekke alle typer behov i offentlig sektor. En mer realistisk tilnærming kan være et økosystem av interoperable tjenester bestående av offentlig eid infrastruktur for særlig kritiske funksjoner, europeiske leverandører og kommersielle tjenester der risikoen er lavere.

Offentlige virksomheter har heller ikke nødvendigvis de samme behovene for skalerbarhet som globale hyperskala-plattformer er utviklet for. For mange tjenester vil stabil drift, kontroll over data, identitet og tilgang være viktigere enn ekstrem skalerbarhet. Det avgjørende er derfor å sikre kontroll over kritiske funksjoner, ikke nødvendigvis å erstatte alle eksisterende tjenester med én statlig plattform.

Tekna vil derfor peke på flere spørsmål som bør avklares før en slik løsning etableres:

- hva som konkret menes med en «nasjonal sky»
- hvilke behov og problemstillinger løsningen skal adressere
- hvilke aktører som skal bruke den og i hvilke situasjoner
- hvordan eierskap, drift og finansiering skal organiseres over tid

De store skyleverandørene har utviklet svært integrerte systemer der management-programvare, maskinvare, nettverk og lagring er optimalisert som én helhetlig arkitektur. Dette gjør det krevende å etablere løsninger som kan levere tilsvarende skalerbarhet, utviklingshastighet og driftsstabilitet.

Tekna mener eventuelle nasjonale løsninger først og fremst bør prioritere systemer som håndterer sensitive persondata, kritiske registre og identitetsforvaltning.

Tekna vil også understreke at beredskap ikke bare handler om hvor tjenester ligger, men om evnen til å flytte tjenester mellom ulike leverandører. Evnen til å gjennomføre slike endringer raskt kan være avgjørende i en krisesituasjon.

3. Stortinget ber regjeringen utvikle en konsesjonsordning for innsamling, bruk og lagring av både offentlige data og persondata for kommersielle aktører. En slik konsesjonsordning må fastsette krav til hvilke data som kan brukes, til hvilke typer formål, hvor og hvordan de lagres, og om og hvordan de kan deles med ulike tredjeparter.

Tekna er kritisk til forslaget om å etablere en konsesjonsordning for innsamling og bruk av data.

Personvernregelverket i Europa bygger på et ansvarlighetsprinsipp der virksomhetene selv har ansvar for å dokumentere behandlingsgrunnlag, nødvendighet og risiko ved behandling av persondata. Dette prinsippet er sentralt i GDPR.

Tekna mener en statlig konsesjonsordning for bruk av data kan komme i konflikt med dette prinsippet og dermed bidra til å svekke den systematikken personvernregelverket bygger på.

Tekna vil også understreke at det i praksis er svært vanskelig å håndheve tekniske begrensninger på hvordan data brukes etter at tilgang er gitt til en aktør. Når data først er gjort tilgjengelig, finnes det i mange tilfeller ingen teknisk mekanisme som fullt ut kan garantere at data ikke brukes til andre formål enn det som opprinnelig var forutsatt.

Dersom hensikten med forslaget er å adressere maktkonsentrasjon i datamarkeder, mener Tekna dette bør behandles mer eksplisitt som et spørsmål om konkurranse, datatilgang og plattformmakt. Utviklingen innen kunstig intelligens gjør at tilgang til store datamengder i økende grad blir en strategisk ressurs. Regulering av datatilgang bør derfor vurderes i lys av både personvern, innovasjon og konkurranseforhold.

Tekna mener derfor at det er mer hensiktsmessig å styrke etterlevelsen av eksisterende regelverk, herunder GDPR, enn å etablere nye konsesjonsordninger som kan skape uklarhet om ansvar og håndheving.

Tekna vil også peke på at Norge har et handlingsrom til å ta i bruk nye og hensiktsmessige regelverk tidligere, også før de er endelig vedtatt i EU. En mer proaktiv tilnærming kan bidra til å styrke kontroll over data og redusere sårbar avhengighet av eksterne aktører.

4. Stortinget ber regjeringen utarbeide en nasjonal exit-strategi for utfasing av store internasjonale kommersielle IT-plattformer, slik som Microsoft 365, i statsforvaltningen og i virksomheter med kritiske samfunnsfunksjoner, slik danske myndigheter gjør, med sikte på overgang til nye systemer fortløpende i løpet av 2026.

Tekna støtter forslaget om å utvikle en nasjonal exit-strategi for å redusere leverandørlåsing i offentlig sektor og styrke evnen til å håndtere bortfall av kritiske digitale tjenester. Etter Teknas vurdering er dette et riktig grep for å redusere sårbar avhengighet av enkeltleverandører og styrke den digitale beredskapen.

Tekna mener det er mulig å lykkes med en slik omstilling. Det finnes allerede både skybaserte og åpne alternativer til dagens løsninger, herunder løsninger

basert på åpen kildekode, som for eksempel LibreOffice, der virksomheten i større grad tar ansvar for drift og kontroll. Begge tilnærminger kan være relevante å utforske og teste i offentlig sektor. For mindre komplekse eller standardiserte bruksområder kan slike løsninger også være en hensiktsmessig strategi i ordinær drift. Reduserte lisenskostnader kan i slike tilfeller bidra til å helt eller delvis kompensere for omstillingskostnader.

Det er også grunn til å forvente økt utvikling og konkurranse i det europeiske markedet i årene som kommer. En nasjonal exit-strategi kan bidra til å akselerere denne utviklingen ved å skape forutsigbar etterspørsel og tydelige krav fra offentlig sektor.

Erfaringene fra Danmark og samarbeidsmodeller som OS2 viser at redusert leverandøravhengighet ikke bare er mulig, men allerede er i utvikling, og at effekten kan forsterkes gjennom tettere nordisk og europeisk samarbeid.

Samtidig vil Tekna understreke at en slik omstilling vil kreve tid, kompetanse og gradvis oppbygging av alternative løsninger og arkitekturer. En exit-strategi bør derfor først og fremst forstås som et langsiktig beredskapstiltak for å redusere risiko. Det overordnede målet bør være å redusere systemisk leverandøravhengighet og sikre at offentlig sektor har arkitekturer og kompetanse som gjør det mulig å migrere til alternative løsninger dersom det blir nødvendig.

Vår avhengighet av etablerte plattformer har utviklet seg over lang tid, og i mange tilfeller er disse systemene tett integrert i organisasjonenes arbeidsprosesser og øvrige digitale løsninger.

Leverandørlåsing oppstår ikke bare gjennom selve programvaren, men også gjennom rekke strukturelle forhold, blant annet:

- integrasjoner mot andre systemer
- organisasjonsspesifikke tilpasninger
- identitets- og tilgangssystemer
- bruk av plattformspesifikke tjenester i skymiljøer

Tekna vil også peke på at ulike teknologiske lag har ulike tidshorisonter for migrering. Kontorstøtte- og samhandlingsverktøy kan i mange tilfeller erstattes relativt raskt, mens mer grunnleggende infrastrukturlag som skytjenester, databaser og analyseplattformer ofte er mer komplekse å flytte.

Tekna mener derfor at en hensiktsmessig tilnærming vil være å utvikle strategier for exit-beredskap, der offentlig sektor gradvis bygger opp arkitekturer og kompetanse som gjør det mulig å bytte leverandør dersom det blir nødvendig.

Dette kan blant annet innebære:

- pilotprosjekter med alternative løsninger

- økt bruk av åpne standarder og portabilitet av data
- arkitekturvalg som reduserer avhengigheten av plattformspesifikke tjenester.

En slik tilnærming kan bidra til å redusere risikoen knyttet til leverandøravhengighet, samtidig som stabil drift av eksisterende systemer ivaretas.

5. Stortinget ber regjeringen redegjøre for hvordan de bedre vil følge opp GDPR og sikre at sensitiv og samfunnskritisk informasjon om innbyggere utelukkende skal behandles i løsninger som er under norsk eller europeisk jurisdiksjon.

Tekna støtter at spørsmålet om jurisdiksjon og kontroll over data vurderes grundig. For sensitiv og samfunnskritisk informasjon mener Tekna at det bør være et klart mål at behandling skjer i løsninger som er under norsk eller europeisk jurisdiksjon.

EU-domstolens Schrems II-dom illustrerer hvordan forskjeller i overvåkningslovgivning kan skape grunnleggende utfordringer for overføring av persondata mellom jurisdiksjoner. Når sensitive personopplysninger behandles i infrastrukturer underlagt fremmede staters lovgivning, kan dette også reise spørsmål om rettssikkerhet for norske borgere.

Kontroll over data handler ikke bare om hvor data lagres fysisk, men også om hvilken jurisdiksjon leverandørene er underlagt og hvem som har tilgang til systemene.

Kontroll over identitetsforvaltning, tilgangssystemer og krypteringsnøkler er sentrale elementer for å sikre reell kontroll over data.

6. Stortinget ber regjeringen redusere leverandørlåsing ved å utarbeide regler for offentlig innkjøp av IT-løsninger som bruker åpne standarder og åpen kildekode med universell utforming og muliggjør interoperabilitet i offentlig sektor.

Tekna støtter tiltak som reduserer leverandørlåsing i offentlig sektor. Tekna vil samtidig peke på at kravet om universell utforming først og fremst er relevant for brukerrettede tjenester. For enkelte typer infrastrukturløsninger kan andre hensyn, som interoperabilitet, portabilitet og sikker arkitektur, være mer direkte relevante for å redusere leverandørlåsing.

Leverandørlåsing oppstår ofte gjennom proprietære teknologier, filformater og API-er. Krav om åpne standarder og interoperabilitet i offentlige anskaffelser er derfor et av de mest effektive virkemidlene for å redusere teknologisk avhengighet.

Åpen kildekode kan også bidra til større fleksibilitet og samarbeid på tvers av offentlig sektor, særlig dersom offentlige virksomheter også bidrar aktivt til

videreutvikling av slike løsninger.

7. Stortinget ber regjeringen styrke og videreutvikle interkommunale samarbeid og oppgavefellesskap som utvikler digitale løsninger for offentlig sektor, basert på åpne kildekoder og standarder.

Tekna støtter intensjonen om å styrke samarbeid om utvikling av digitale løsninger i offentlig sektor. Samtidig mener Tekna at perspektivet bør være bredere enn kun interkommunalt samarbeid.

Etter Teknas vurdering bør man i større grad legge til rette for samarbeid mellom offentlige virksomheter, interkommunale samarbeid og oppgavefellesskap i både statlig og kommunal sektor. Offentlig sektor utvikler allerede en rekke digitale løsninger og teknologiplattformer som kan ha verdi også for andre virksomheter.

Flere statlige virksomheter har i dag utviklet robuste teknologiplattformer og utviklingsmiljøer som i større grad kan fungere som felles plattformer for andre deler av offentlig sektor. Eksempler kan være NAIS-plattformen i NAV, IT-plattformen til Nasjonalbiblioteket eller løsninger utviklet av Brønnøysundregistrene.

Tekna mener derfor det bør legges til rette for større grad av gjenbruk av teknologi, kode og plattformer på tvers av offentlig sektor. Dette kan bidra til bedre ressursutnyttelse, sterkere fagmiljøer og mer robuste digitale løsninger.

Samarbeid om åpne standarder og åpen kildekode kan i denne sammenhengen være et viktig virkemiddel for å legge til rette for slik deling og videreutvikling av løsninger.

Danmark har for eksempel etablert samarbeidsorganisasjonen OS2, som støtter kommuner i utvikling og bruk av åpne kildekode-løsninger basert på åpne standarder. Ifølge OS2 samarbeider rundt 84 prosent av danske kommuner om slike løsninger. Dette illustrerer hvordan samarbeid om åpne teknologiplattformer kan bidra til mer effektiv utvikling, sterkere fagmiljøer og bedre gjenbruk av digitale løsninger i offentlig sektor.

8. Stortinget ber regjeringen ta nødvendige grep for å samarbeide tettere med nordiske og europeiske land om felles digitale løsninger og beredskap, hvor åpne kildekoder og digital suverenitet over digital infrastruktur er førende for samarbeidet.

Tekna mener nordisk og europeisk samarbeid er avgjørende for å styrke digital suverenitet. Digitale infrastrukturer og teknologimarkeder er i økende grad globale. For små land vil samarbeid derfor være avgjørende for å utvikle

robuste alternativer til globale plattformer.

Dette handler ikke om å isolere Norge fra det globale teknologimarkedet, men om å redusere sårbare avhengigheter og sikre kontroll over kritiske digitale funksjoner i samfunnet. Offentlig sektor vil fortsatt være avhengig av internasjonale teknologileverandører, men bør samtidig utvikle arkitekturer, kompetanse og samarbeidsformer som gjør det mulig å bytte leverandør dersom det blir nødvendig.

Tekna mener derfor at digital suverenitet først og fremst bør forstås som evnen til å opprettholde kritiske samfunnsfunksjoner også dersom enkeltleverandører eller tjenester faller bort.

For et lite land vil dette i stor grad være avhengig av samarbeid. Tekna mener derfor at nordisk og europeisk samarbeid om digital infrastruktur, åpne teknologiplattformer og kompetanseutvikling vil være avgjørende for å styrke den digitale robustheten i årene som kommer.

Et sterkere europeisk samarbeid kan bidra til større teknologimiljøer, delte utviklingskostnader og mer robuste digitale infrastrukturer.

Tekna mener derfor Norge bør delta aktivt i europeiske initiativer knyttet til digital infrastruktur, cybersikkerhet og åpne teknologiplattformer.